

# Notice of Allowability

Application No.

09/751,899

Examiner

Tony Mahmoudi

Applicant(s)

GRAWROCK, DAVID W.

Art Unit

2165

## -- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to the amendment filed on 05-April-06 & the Examiner's Amendment authorized on 10-April-06.
2. ☒ The allowed claim(s) is/are 1-2, 4-9, 11, 15-19, and 21-22, re-numbered as claims 1-16.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a) ☐ All b) ☐ Some\* c) ☐ None of the:
    1. ☐ Certified copies of the priority documents have been received.
    2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
    3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

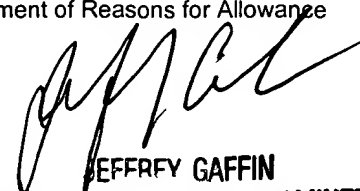
Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
  5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
    - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date \_\_\_\_\_.
    - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

### Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date \_\_\_\_\_
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date 20060410
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other \_\_\_\_\_

  
JEFFREY GAFFIN  
SUPERVISING PATENT EXAMINER  
TECHNOLOGY CENTER 2100

## **DETAILED ACTION**

### ***Remarks***

1. In response to the Amendment filed by the Applicant on 05-April-2006, and in view of the Examiner's Amendment, authorized by the Attorney of Record (details provided below), claims 3, 10, 12-14, 20, and 23 are canceled and claims 1, 4-5, 15, and 19 are amended. Therefore, claims 1-2, 4-9, 11, 15-19, and 21-22 are presently pending in the application, of which, claims 1, 15, and 19 are presented in independent form.

### ***Examiner's Amendment***

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mr. William W. Schaal (Attorney of Record) on 07-April-2006, and via Email on 10-April-2006 (see enclosed Interview Summary, paper No. 20060410.)

### ***Listing of Claims***

The following is a complete listing of the claims in the instant application, as Amended by the Examiner, authorized by the Attorney of Record. This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method comprising:
  - loading a Basic Input/Output System (BIOS) code including a first BIOS area and a second BIOS area, the first BIOS area being a first segment of the BIOS code encrypted with a keying material stored within an internal memory of a trusted platform module of a platform and the second BIOS area being a second segment of the BIOS code encrypted with a combination key;
  - loading an integrity metric including a hash value of an identification information of the platform;
  - authenticating a user of ~~a~~ the platform during a ~~Basic Input/Output System (BIOS)~~ boot process;
  - releasing a first keying material from a token communicatively coupled to the platform after authenticating the user during the BIOS boot process;
  - combining the first keying material with a second keying material internally stored within the platform in order to produce a combination key during the BIOS boot process; and
  - using the combination key to decrypt a second BIOS area to recover a second segment of BIOS code during the BIOS boot process.
2. (Original) The method of claim 1 further comprising:
  - continuing the BIOS boot process.
3. (Cancelled).
4. (Currently Amended) The method of claim ~~3~~ 2, wherein after loading of the BIOS code, the method further comprises:
  - decrypting the first BIOS area to recover the first segment of the BIOS code.

Art Unit: 2165

5. (Currently Amended) The method of claim ~~3~~ 1, wherein the first segment of the BIOS is encrypted with the keying material and static information pertaining to the platform, the static information including the integrity metric.

6. (Original) The method of claim 1 wherein the combination key is a value formed by performing an exclusive OR operation on both the first keying material and the second keying material.

7. (Original) The method of claim 1, wherein authentication of the user is performed through biometrics.

8. (Original) The method of claim 1, wherein the second keying material is stored within internal memory of a trusted platform module.

9. (Original) The method of claim 1, wherein the second keying material is stored within a section of access-controlled system memory of the platform.

10. (Cancelled).

11. (Original) The method of claim 1, wherein the identification information includes a serial number of an integrated circuit device employed within the platform.

12. (Cancelled).

13. (Cancelled).

14. (Cancelled).

15. (Currently Amended) A platform comprising:  
an input/output control hub (ICH);

a non-volatile memory unit coupled to the ICH, the non-volatile memory unit including an integrity metric including a hash value of an identification information of a platform and a Basic Input/Output System (BIOS) code including a first BIOS area and a second BIOS area, the first BIOS area being a ~~an encrypted~~ first segment of the BIOS code encrypted with a second keying material and the second BIOS area being an ~~encrypted~~ a second segment of the BIOS code encrypted with a combination key; and

a trusted platform module coupled to the ICH, the trusted platform module to produce a combination key during a BIOS boot process by combining a first incoming keying material released after authentication of a user of the platform with ~~a~~ the second keying material internally stored within the platform and to decrypt the second BIOS area using the combination key to recover the second segment of BIOS code.

16. (Original) The platform of claim 15, wherein the trusted platform module to further decrypt the first BIOS area to recover the first segment of the BIOS code in an non-encrypted format.

17. (Original) The platform of claim 15 further comprising a hard disk drive coupled to the ICH.

18. (Original) The platform of claim 17, wherein the trusted platform module to further unbind keying material associated with the hard disk drive to access contents stored within the hard disk drive.

19. (Currently Amended) A program loaded into computer readable memory, including at least one of a non-volatile memory and a volatile memory, for execution by a trusted platform module of a platform, the program comprising:

code to decrypt a first Basic Input/Output System (BIOS) area of a BIOS code during a BIOS boot process to recover a first segment of BIOS code, the first BIOS area being the first segment of the BIOS code encrypted with a keying material and an integrity metric including a hash value of an identification information of the platform;

Art Unit: 2165

code to produce a combination key during the BIOS boot process by combining a first incoming keying material released after authentication of a user of the platform with a second keying material internally stored within the trusted platform module; and

code to decrypt a second BIOS area of the BIOS code using the combination key to recover a second segment of the BIOS code during the BIOS boot process, the second BIOS area being the second segment of the BIOS code encrypted with the combination key.

20. (Cancelled).

21. (Original) The program of claim 19 further comprising:

code to unbind keying material associated with a non-volatile storage device for accessing contents stored within the non-volatile storage device.

22. (Previously Presented) The method of claim 5, wherein the static information is a serial number or a hash value of the serial number associated with hardware within the platform.

23. (Cancelled).

#### *Allowance*

3. Claims 1-2, 4-9, 11, 15-19, and 21-22 are allowed over the prior art made of record.

#### *Conclusion*

4. Any inquiries concerning this communication or earlier communications from the examiner should be directed to Tony Mahmoudi whose telephone number is (571) 272-4078. The examiner can normally be reached on Mondays-Fridays from 08:00 am to 04:30 pm.

Art Unit: 2165

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeffrey Gaffin, can be reached at (571) 272-4146.

tm

April 10, 2006